## IN THE CLAIMS:

1-15 (canceled)

1   16. (currently amended) A process for protecting a software product, sent from a server

2 computer to a computer, from unauthorized usage, the process comprising the steps of:

3       generating a first set of parameters from the computer before the software product

4 is encrypted at the server,

5       sending the first set of parameters to the server computer before the software

6 product is encrypted at the server,

7       creating, at the server computer, a single value from the first set of parameters be-

8 fore the software product is encrypted at the server,

9       encrypting, at the server computer, the software product by using the single value

10 as the encryption key,

11       sending the encrypted software product to the computer,

12       encrypting, at the server computer, the single value by using members of the first

13 set of parameters as encryption keys, to form a set of encrypted single values,

14       sending the set of encrypted single values to the computer,

15       generating a second set of parameters from the computer,

16       decrypting members of the set of encrypted single values using members of the

17 second set of parameters as decryption keys,

18       creating, at the computer, from the decrypted members of the set of encrypted

19 single values, the single value, and

20       ~~decrypting~~ decrypting, at the computer, the encrypted software product by using

21 the single value as the decryption key.

1   17. (currently amended) The process of claim 16 wherein the software product comprises

2 ~~ay~~ at least one data file or streaming data or both.

2

1   18. (currently amended) A process for protecting a software product, sent from a server

2   computer to a computer, from unauthorized usage, the process comprising the steps of:

3       generating a first set of parameters from the computer before the software product

4   is encrypted at the server,

5       sending the first set of parameters to the server computer before the software

6   product is encrypted at the server,

7       creating, at the server computer, a single value from the first set of parameters be-

8   fore the software product is encrypted at the server,

9       encrypting, at the server computer, the single value using members of the first set

10   of parameters as encryption keys, to form a set of encrypted _single_values,

11       sending the set of encrypted single values to the computer,

12       sending the software product to the computer,

13       generating a second set of parameters from the computer,

14       decrypting, at the computer, members of the set of encrypted single values by us-

15   ing members of the second set of parameters as decryption keys, and

16       inspecting the decrypted single values, and if enough are identical,

17       authorizing access to the software product at the computer.


1   19. (previously presented) The process of claim 18 wherein the software product com-

2   prises at least one data file or streaming data or both.


1   20. (previously presented) The process of claim 18 further comprising the step wherein if

2   the said decryption yields a quorum of identical single values, then

3       authorizing access to the software product at the computer.


1   Claims 21- 24 (canceled).


3

1    25. (currently amended)  A process for protecting a software product, sent from a server

2    computer to a computer, from unauthorized usage, the process comprising the steps of:

3            generating a first set of parameters from the computer before the software product

4    is encrypted at the server,

5            sending the first set of parameters to the server computer, before the software

6    product is encrypted at the server,

7            creating, at the server computer, a single value from the first set of parameters,

8    before the software product is encrypted at the server,

9            encrypting, at the server computer, the single value by using members of the first

10   set of parameters as the encryption keys, to form a set of encrypted values,

11           sending the set of encrypted single values to the computer,

12           sending the software product to the computer,

13           generating a second set of parameters from the computer,

14           decrypting members of the set of encrypted single values by using members of the

15   second set of parameters as the decryption keys, and

16           <u>inspecting the decrypted single values, and if enough are identical,</u>

17           authorizing the execution of the software product on the computer.


1    26 (previously presented)  The process of claims 25 further comprising the step wherein

2    if the said decryption yields a quorum of identical single values, then

3            authorizing the execution of the software product on the computer.


1    27. (previously presented)  The process of claim 25 wherein the software product com-

2    prises at least one data file or streaming data or both.

3

1    Claims 28 – 39 (canceled).

2


4